Published and Copyright (c) 1999 - 2015
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1721 06/05/15

~ Politwoops Is Shut Down ~ People Are Talking! ~ Supreme Court Ruling!
~ Personal Data Exposed! ~ Pirate Bay'er Released! ~ XCOM 2 This Fall!
~ Fallout 4 Is Revealed! ~ Beijing's Hack Response ~ Win 10 This Summer!

~ Electronics Search Bill ~ Charge People for Email ~ Win 10 Pricing!

-* Focus on China in Fed Hack! *-
-* Video Game Hall of Fame First Class! *-
-* Obama Signs USA Freedom Act, Clips the NSA *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

I have to admit, this week's issue was looking kind of shaky until earlier today! Thankfully, A-ONE's best contributor - Fred Horvat - saved the day wil a number of articles that he thought might be interesting to include in the magazine. While a number of his stories had already been included, there were quite a few others that made the difference in whether or not we had sufficient material for this issue. Thanks again, Fred - you saved the day again!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Fallout 4 Officially Revealed!
""""""""""""""""""""""""""""""""" 'XCOM 2' Infiltrates PCs in November!
Video Game Hall of Fame's First Class
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

Fallout 4 Officially Revealed, Internet Explodes

Get ready to head back into the wasteland.

After innumerable hoax reports and countless months of wishful thinking, fans of the post-apocalyptic Fallout series finally have something worth staring at. Bethesda has confirmed that Fallout 4 is, in fact, real.

The publisher posted a countdown clock Tuesday. A trailer went live Wednesday morning.

As far as teasers go, it’s got pretty much everything you could ask for: mystery, a haunting version of The Ink Spots’ "It’s All Over But The Crying," hints of the game’s future and past, creepy mutants, an awesome dog, and, perhaps most importantly, the hair-raising narration of series mainstay Ron Perlman, including his iconic line "War. War never changes."

The video also seemingly confirms a few rumors. Fallout 4 is at least partially set in Boston, judging by the inclusion of a Paul Revere statue and Fenway Park in the trailer. And it hints just hints that we might be able to explore the world of Fallout in the days before the atomic apocalypse that plays such an important role in the game’s fiction (though certainly, that could just be a storytelling device of the trailer).

Hoping to see Dogmeat again? We’re not sure if it’s him, but a German Shepherd is the star of the trailer, sniffing around the desolate remains of a once-happy home before meeting up with his human companion. Please let us play as the dog. Please.

That s up in the air, but here’s what’s certain. The game is being developed for the Xbox One, PlayStation 4 and PC. Game maker Todd Howard, who led the creation of the immensely popular Fallout 3 and Bethesda s equally-vaunted The Elder Scrolls series, is once again in charge.

 We know what this game means to everyone, Howard said in a statement. The time and technology have allowed us to be more ambitious than ever. We ve never been more excited about a game, and we can t wait to share it.

The news swept across the web like wildfire. Within an hour of the announcement, ’Fallout 4’ was Twitter’s top trending topic. ’Bethesda’ is in the top ten. Well done, marketing people.

When will be get to play it? Right now, there’s no telling, though we suspect Bethesda will give us a little more clarity at its pre-E3 media briefing, which will be held (and streamed) at 7:00 pm PST June 14. Fans, though, can pre-order the game on its official website starting today.

’XCOM 2’ Infiltrates PCs in November

Prepare for permadeath. XCOM 2, the sequel to 2012’s wonderfully rich strategy game XCOM: Enemy Unknown, is due to hit PC in November. XCOM 2 comes from publisher 2K and developer Firaxis Games, the very same team behind Enemy Unknown. They’ve been teasing a big announcement with a website for the Advent Administration, a futuristic government that advertises gene therapies and other technologies that rid humans of all illness - but the site has been hacked with messages that suggest all is not as rosy as it seems.

In XCOM 2, it’s 20 years in the future and aliens control the Earth. The XCOM special forces have gone guerrilla and "must strike back to reclaim control of Earth and free mankind from the aliens’ rule," 2K says. So far, XCOM 2 is confirmed for PC only, with no mention of consoles or mobile. XCOM 2 is a continuation of the XCOM franchise, which has been around since 1993. XCOM as a series is historically acclaimed for its

deep turn-based strategy gameplay and heart-breaking use of permadeath - meaning once characters die, they’re gone forever.

Even through the tears over fallen comrades, Joystiq adored XCOM: Enemy Unknown, calling it "an exemplary turn-based strategy game." Three years later, we’ll see if XCOM 2 continues to carry the tactical torch.

Fun, Colorful Shooter Splatoon Paints With A Purpose

Leave it to Nintendo to find harmony in the words family-friendly and competitive online shooter. But that unlikely pairing is exactly what you get in Splatoon. You also get a helluva good time.

Perhaps more notable than the fact that Nintendo released a third-person shooter for the Wii U is the fact that this game doesn t star any familiar faces. Splatoon is the first brand new character-driven franchise the company has created in over 14 years (the last one being the original Pikmin on the Gamecube). No Mario, no Yoshi, no Donkey Kong, nada. Nintendo is asking the rookie to stand on its own two tentacles, sans the cozy surety of an iconic logo, and help breathe life into the struggling Wii U console.

Are they nuts? As it turns out, they re just being Nintendo. Though its inkwell runs a bit dry, Splatoon is a fun, innovative game that manages to be both everything and nothing you d expect from the video game pioneer.

Its main mode, Turf Wars, boasts a wonderful premise: cover the world with ink. Two teams of four face off on a map, but rather than go for headshots, the goal is to drench as much ground with your team s color as possible. While taking out enemies is well and good, it s secondary to making a mess of the map.

There s another benefit to spraying your ink everywhere. Splatoon s new characters   the Inklings   aren t just xtreme, paint-crazy teens. In human form, your Inkling runs around on two legs. But press a button and the little weirdo turns into a squid, able to refill ammo, hide, and nimbly swim through your team s ink.

With these basic tools in its tank, a game of Splatoon is a surprisingly strategic affair. Do you charge ahead and start splattering? Lay some paint pathways for your teammates and lurk defensively? A favorite technique is to hide in a vast ink pool and pop out like a trapdoor spider to douse an unsuspecting enemy in gaudy green goo. It s truly a new kind of shooter.

It also makes great use of the Wii U Gamepad. There s a learning curve here   the motion sensors on the Gamepad are a little sensitive   but once you get the hang of aiming, swimming, and shooting, it gels. Better still, the Gamepad doubles as a handy top-down map of the inky battlefield. Not sure where to spray? Peek at the map and start painting.

The better you play, the faster you level up and earn coins to spend in Inkopolis. Splatoon s city functions as its main hub, housing the curious vendors hawking new guns and gear. Outfitting your Inkling in new duds tweaks skills, and the more you use a piece of clothing, the more bonuses you ll unlock. The guns come in a handful of styles, but as you level up you ll gain access to modified versions that include interesting

combinations of sub-weapons. I found myself addicted to the not-so-nuanced Splat Roller, which is good for up close combat and coating the ground in a thick layer of ink. But snipers, machine gunner, and shotgun types will all find perfectly suitable Splatoon versions.

Mastering Splatoon s mechanics takes some time, and while that s best spent online, there s a short, Super Mario-lite solo campaign here as well. You re tasked with tracking down the prized electric zapfish, which have been stolen by the nefarious Octarians. That s really just an excuse to send you through a variety of fun, imaginative platform levels that make use of the ink in interesting ways. You ll inflate giant sponges by pumping them full of paint, ride inky geysers, and battle imposing bosses. It s good stuff, but over too quickly to really sink in.

Why kid squids? Why zapfish? Why ink? Why not? Splatoon channels an arcadey, Technicolor playfulness that s been buried beneath years of brown and gray shooters, tapping into a part of the gamer brain that in many ways died with the Sega Dreamcast. Haphazardly flinging paint like a rifle-toting Jackson Pollock is its own reward. Heck, this might be the first shooter where shooting directly at the ground is a good thing.

And no matter how splendidly or terribly you paint, Splatoon looks awesome. Like most Nintendo games, it runs fast and smooth, and boasts a poppy punkish soundtrack that manages to toe the line between irritating and infectious. Reveling in its vibrant palette, Splatoon is a breath of fresh air in an ocean of dour, overly serious military-themed shooters.

Unfortunately, things get a bit sticky when it comes to the game s online play. In spite of Splatoon s team-based nature, there s no voice chat. On one hand, I get it. Nintendo wants to create a safe space for players of all ages, and getting hollered at by an aggro jerk because you re not doing exactly the right thing at the right time doesn t jibe.

But what about when you re the aggro jerk? I can t count the number of times I watched helplessly as my terrible team opted to rush off to kill the bad guys and forget to paint much of anything, or fail to help take down a troublesome sniper dominating the map. What s an aggro jerk to do?

Shut up and take it, that s what. With no way to communicate beyond passive-aggressively firing ink at the godless sky, Splatoon s team dynamics often feel more like luck of the draw than any sort of tactical affair. It s a great game when you get a great team. It s pretty frustrating when you don t.

Questionable matchmaking doesn’t help. Perhaps there’s a dearth of players out there, but all too frequently, I find myself on the wrong end of lopsided teams. Maybe split up the two level 20s and give the rest of us level 11s a chance? I’m no good at new math, but this can’t be that hard.

There s also the issue of content. Splatoon launched with only five maps, and while Nintendo has already released one more, it still feels thin. At level 10 you unlock the ability to play in Ranked Battles, opening up the fun Zone Control game mode, but two modes in an online shooter? Splatoon s meager maps and modes come up short.

But comparing Splatoon to Call of Duty is kind of ridiculous. Nintendo is painting on its own canvas here, not trying to mimic the experience found in other games, and in that, they ve succeeded. Splatoon isn t quite a masterpiece, but it s a promising start for a colorful new artist.

=~=~=~=

->A-ONE Gaming Online - Online Users Growl & Purr!
"""""""""""""""""""""

’Pong,’ ’Tetris’ Make Video Game Hall of Fame’s First Class

The first inductees into the new World Video Game Hall of Fame include "Pong," the game that introduced millions to electronic play, "Doom," which triggered a debate over the role of games and violence in society, and "Super Mario Bros.," whose mustachioed hero has migrated to everything from fruit snacks to sneakers.

The first six games to enter the hall of fame cross decades and platforms, but all have impacted the video game industry, popular culture and society at large, according to the new hall at The Strong museum in Rochester, where the games were enshrined Thursday.

Joining "Pong," launched in 1972, "Doom," from 1993, and 1985’s "Super Mario Bros." are arcade draw "Pac-Man" (1980); Russian import "Tetris" (1984); and "World of Warcraft" (2004), which has swallowed millions of players into its online virtual universe.

The newly created World Video Game Hall of Fame pays homage to an industry that rivals Hollywood in the entertainment pecking order. The Strong, which bills itself as the national museum of play and also houses the National Toy Hall of Fame, has been preserving and collecting games and artifacts for years through its International Center for the History of Electronic Games.

"Electronic game play is increasingly influential and important," Strong President and Chief Executive G. Rollie Adams said. "It’s changing how we play, how we learn and how we connect with each other across boundaries of geography and culture."

The inaugural hall of fame class was recommended by a panel of judges made up of journalists, scholars and other experts on the history and impact of video games. They chose from among 15 finalists that also included: "Angry Birds," ’’FIFA," ’’The Legend of Zelda," ’’Minecraft," ’’The Oregon Trail," ’’Pokemon," ’’The Sims," ’’Sonic the Hedgehog" and "Space Invaders."

Nominations for the hall can come from anyone and be from any platform arcade, console, computer, handheld or mobile. But they must have had a long stretch of popularity and left a mark on the video game industry or pop culture.

"Doom," for example, introduced the idea of a game "engine" that separated the game’s basic functions from its artwork and other aspects, but even more significantly was one of the early games cited in the debate that continues today over whether violent games inspire real-life aggression.

"World of Warcraft," is the largest MMORPG "massively multiplayer online role-playing game" ever created. As of February, it had more than 10 million subscribers, represented by avatars they create, according to The Strong.

Sixteen-year-old gamer Shaun Corbett, of Rochester, said after the induction ceremony that he was expecting "Doom," ''Super Mario Bros." and "Pac-Man" to get in.

"'Tetris' I wasn't expecting but I can see where they're coming from. It made puzzle games popular," Corbett said.

He said his fascination with video games started with Pokemon.

"I enjoyed watching the show. I enjoyed playing the card game," he said. "I got the video game on the Game Boy Advance for Christmas when I was 7 and I just have a lot of good memories of playing it with my cousins, my parents showing me how it worked."

More than 150 million Americans play video games, according to the Entertainment Software Association, and 42 percent play for at least three hours a week. In 2014, the industry sold more than 135 million games and generated more than $22 billion in revenue, according to the ESA.

Nominations for the hall of fame's class of 2016 are open from now through the end of March.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

China in Focus As Cyber Attack Hits Millions of U.S. Federal Workers

Hackers broke into U.S. government computers, possibly compromising the personal data of 4 million current and former federal employees, and investigators were probing whether the culprits were based in China, U.S. officials said on Thursday.

Cyber investigators linked the breach to earlier thefts of healthcare records from Anthem Inc, the second largest U.S. health insurer, and Premera Blue Cross, a healthcare services provider.

In the latest in a string of intrusions into U.S. agencies' high-tech systems, the Office of Personnel Management (OPM) suffered what appeared to be one of the largest breaches of information ever on government workers. The office handles employee records and security clearances.

A U.S. law enforcement source told Reuters a "foreign entity or government" was believed to be behind the cyber attack. Authorities were looking into a possible Chinese connection, a source close to the matter said.

A Chinese Foreign Ministry spokesman said such accusations had been frequent of late and were irresponsible. Hacking attacks were often cross-border and hard to trace, he said.

The FBI said it was investigating and aimed to bring to account those responsible.

Several U.S. states were already investigating a cyber attack on Anthem in February that a person familiar with the matter said is being examined for possible ties to China.

John Hultquist of Dallas-based iSight Partners told Reuters that the latest attack on OPM and the earlier breaches at Anthem and Premera Blue Cross appear to have been the work of cyber espionage hackers working on behalf of a state, not those focused on cybercrime.

He said they may have widened their net to gather personally identifiable information for more elaborate, finely-tuned attacks in the future. "This is usually done by criminals, but based on their behavior, we believe these are espionage actors," said Hultquist.

OPM detected new malicious activity affecting its information systems in April and the Department of Homeland Security said it concluded at the beginning of May that the agency’s data had been compromised and about 4 million workers may have been affected.

The agencies involved did not specify exactly what kind of information was accessed.

The breach hit OPM’s IT systems and its data stored at the Department of the Interior’s data center, a shared service center for federal agencies, a DHS official said on condition of anonymity. The official would not comment on whether other agencies’ data had been affected.

OPM had previously been the victim of another cyber attack, as have various federal government computer systems at the State Department, the U.S. Postal Service and the White House.

Chinese hackers were blamed for penetrating OPM’s computer networks last year, and hackers appeared to have targeted files on tens of thousands of employees who had applied for top-secret security clearances, the New York Times reported last July, citing unnamed U.S. officials.

"The FBI is working with our inter-agency partners to investigate this matter," the bureau said in a statement. "We take all potential threats to public and private sector systems seriously, and will continue to investigate and hold accountable those who pose a threat in cyberspace."

The U.S. government has long raised concerns about cyber spying and theft emanating from China and has urged Beijing to do more to curb the problem.

Chinese Foreign Ministry spokesman Hong Lei told a regular daily news briefing in Beijing that China hoped the United States would have more trust and cooperate more.

"Without first thoroughly investigating, always saying that ’it’s possible’, this is irresponsible and unscientific," said Hong.

There was no comment from the White House.

Since the intrusion, OPM said it had implemented additional security precautions for its networks. It said it would notify the 4 million employees and offer credit monitoring and identity theft services to those affected.

"The last few months have seen a series of massive data breaches that have affected millions of Americans," U.S. Representative Adam Schiff, the ranking Democrat on the House Permanent Select Committee on Intelligence, said in a statement.

Tens of millions of records may have been lost in the attacks on Anthem and Premera Blue Cross.

iSight’s Hultquist said similar methods, servers and habits of the attackers pointed to one state-sponsored group being responsible for all three breaches.

The largest federal employee union said it was working with the administration to ensure measures were taken to secure the personal information of affected employees. "AFGE will demand accountability," American Federation of Government Employees President J. David Cox Sr. said in a statement.

In April, President Barack Obama responded to a growing rash of attacks aimed at U.S. computer networks by launching a sanctions program to target individuals and groups outside the United States that use cyber attacks to threaten U.S. foreign policy, national security or economic stability.

The move followed indictments of five Chinese military officers who were charged with economic espionage. U.S. officials also pointed the finger directly at North Korea for a high-profile attack on Sony over a film spoof depicting the assassination of North Korea’s leader.

China has routinely denied accusations by U.S. investigators that hackers backed by the Chinese government have been behind attacks on U.S. companies and federal agencies.

U.S. military officials have become increasingly vocal about cyber espionage and attacks launched by China, Russia and other rivals. A Pentagon report in April said hackers associated with the Chinese government repeatedly targeted U.S. military networks last year seeking intelligence.

Hack Exposes Personal Data of 4 Million Federal Workers

Officials suspect hackers gained the personal data of 4 million current and former federal employees.Image by Dennis Skley, CC BY-ND 2.0

A cyberattack on the US government’s personnel office compromised the data of up to 4 million current and former federal employees, officials said Thursday.

The FBI said it is investigating a hack of network security at the Office of Personnel Management. Federal officials suspect Chinese hackers are behind the data breach, believed to be the largest in a recent wave of

attacks targeting federal agencies, according to The Wall Street Journal.

"The FBI is working with our interagency partners to investigate this matter," the FBI said in a statement. "We take all potential threats to public and private sector systems seriously, and will continue to investigate and hold accountable those who pose a threat in cyberspace."

The Chinese consulate in San Francisco did not immediately respond to a request for comment.

Investigators told the Journal that the hack, detected in April, is believed to be separate from an attack detected last year. The New York Times reported last year that Chinese hackers worked their way into US government servers in March 2014 in an attempt to steal information on thousands of federal employees with top-secret clearance.

Computer hacking is a sore subject between the US and China. Both countries have publicly accused each other of breaking in to servers to steal information.

In May 2014, the US Justice Department filed charges against five alleged Chinese military hackers. They are charged with hacking American corporations and stealing information. China has denied the allegations.

The security breach is the latest in a recent wave of cyberattacks that have targeted government agencies and that are suspected of originating overseas. After a security breach of an unclassified network used by White House advisers was revealed last year, suspicion immediately fell on hackers thought to be working for the Russian government.

The National Oceanic and Atmospheric Administration, which includes the National Weather Service, also revealed last year that four of its websites were compromised by an "Internet-sourced attack." Chinese government hackers were suspected in that attack, as well as one on the US Postal Service, in which data for more than 800,000 employees was compromised.

The Office of Personnel Management is the federal government’s human resources department, responsible for conducting the majority of the government’s background checks for security clearances, among other responsibilities. The agency said it detected the intrusion in April and has since added additional security defenses to its network.

"The intrusion predated the adoption of the tougher security controls," the OPM said in a statement.

The OPM also said it plans to notify approximately 4 million individuals whose personally identifiable information may have been compromised in the breach. The agency also warned that additional exposure of personal information may still come to light.

"We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted," OPM Director Katherine Archuleta said in a statement.

Data Obtained in U.S. Government Hack Dates Back to 1985

Data stolen in the recent hack of U.S. government computers includes security clearance information and background checks dating to 1985, a U.S. official said, underlining the far-reaching scale of one of the largest known thefts of federal government data.

"This is deep. The data goes back to 1985. This means that they potentially have information about retirees, and they could know what they did after leaving government," said the official, speaking on condition of anonymity.

Access to information from the breach at Office of Personnel Management computer networks, such as birthdates, Social Security numbers and bank information, could help hackers test potential passwords to other sites, including those containing information about critical weapons systems, said the official.

"That could give them a huge advantage."

Beijing Calls Reports China Involved in US Hack ’Irresponsible’

Beijing on Friday labelled as "irresponsible" reports that Chinese hackers were behind a massive cyber-attack on personal data of millions of current and former US federal employees.

The US government on Thursday said that hackers accessed the personal data of at least four million current and former federal employees. Officials told US media that China was suspected.

"Cyber-attacks are generally anonymous and conducted across borders and their origins are hard to trace," foreign ministry spokesman Hong Lei said at a regular briefing.

"Not to carry out a deep investigation and keep using words such as ’possible’ is irresponsible and unscientific," he added.

"As a result of the incident," uncovered in April, the US Office of Personnel Management said it "will send notifications to approximately four million individuals."

It added that additional exposures "may come to light."

The government’s personnel department handles hundreds of thousands of sensitive security clearances and background investigations on prospective employees each year.

It was not immediately clear whether the hack affected President Barack Obama, other senior government officials or the intelligence community.

The Washington Post and other US media cited government officials as saying that Chinese hackers were behind the breach.

"We have seen a lot of media reports and opinions like this recently," Hong said.

The Chinese embassy in Washington countered that such attacks would not

be allowed under Chinese law.

"Chinese laws prohibit cyber-crimes of all forms. China has made great efforts to combat cyber-attacks in accordance with Chinese laws and regulations," embassy spokesman Zhu Haiquan said.

US Admiral Michael Rogers, who heads the National Security Agency and US Cyber Command, has said that future attacks could prompt a response with conventional weapons.

The FBI and Department of Homeland Security are said to be leading an investigation into the attack. The FBI in a statement said it "will continue to investigate and hold accountable those who pose a threat in cyber-space."

The government said it will, through a third party, offer $1 million in identity theft protection services at no cost.

"Protecting our federal employee data from malicious cyber-incidents is of the highest priority," Office of Personnel Management director Katherine Archuleta said.

Her agency said the intrusion may have begun late last year and "predated the adoption of the tougher security controls".

The new measures include restricting remote access, screening business connections and deploying anti-malware software.

The incident is the latest in a series of major breaches that have shown the vulnerability of the federal government.

Last year Russian hackers are believed to have accessed unclassified computer systems at the White House and State Department.

Hackers stole information on 100,000 taxpayers from online computers of the US Internal Revenue Service.

The United States has struck an increasingly strident tone about cyber-attacks in recent months.

Admiral Michael Rogers, who heads the National Security Agency and US Cyber Command, has said that future attacks could prompt a response with conventional weapons.

In February, US Director of National Intelligence James Clapper said a steady stream of low-level cyber-attacks posed the most likely danger to the United States, rather than a potential digital "armageddon."

Obama has ranked China and Russia’s cyber-attack capabilities as "very good," Iran’s as "good," and North Korea’s as not "particularly good."

China operates a vast domestic security and surveillance apparatus.

In a recent white paper, Beijing said it would "expedite the development of a cyber-force" within the People’s Liberation Army.

In 2013, US Internet security firm Mandiant said its hundreds of investigations showed that groups hacking into US newspapers, government agencies, and companies "are based primarily in China and that the Chinese government is aware of them".

One group, it said, was believed to be a branch of the People's Liberation Army called Unit 61398, and digital signatures from its cyber-attacks were traced back to a building in Shanghai.

Last year, five members of the unit were indicted by US federal prosecutors on charges of stealing information from companies, including nuclear plant manufacturer Westinghouse, SolarWorld and US Steel.

China is increasingly concerned about US cyber-spying and has ordered many government departments to avoid using foreign technology.

Obama Signs USA Freedom Act into Law, Clipping NSA's Powers

President Obama on Tuesday signed into law the USA Freedom Act.

Some are calling it a significant scaling back of national security policy formed after the 11 September 2001 terrorist attacks, while others are saying that it's at least a good first step in that it means the NSA will be slightly inconvenienced in its spying and there will be a smidgen more accountability and transparency for it and the Foreign Intelligence Surveillance Act (FISA) court.

With the passage of the Freedom Act, US lawmakers resurrected the three spying-centric Patriot Act provisions that presidential candidate Senator Rand Paul single-handedly forced into retirement when those provisions expired at midnight on Monday morning.

The three renewed provisions:

Section 215 of the Patriot Act. This is the business records provision that supports the NSA's bulk collection of telephone records, which has resulted in the agency having collected the phone records of millions of US persons not suspected of any crime.

Under the new legislation, the bulk phone metadata will be taken out of the hands of the NSA and will instead stay with the telecoms.

The NSA can still get at it with the FISA Court's say-so, as long as the government says it has a reasonable suspicion that a target's phone data is relevant to a terror investigation, and that at least one party to a given call is overseas.

The "lone wolf" provision. This allows US intelligence and law enforcement agencies to target surveillance at suspected terrorists who are acting alone without any direct ties to terrorist groups or rogue nations.

This amendment to the Patriot Act specifically says that it doesn't apply to US citizens, and White House officials claim that it's never actually been used.

The "roving wiretap" provision. This renewed provision allows federal spies to monitor a suspected terrorist person rather than a specific phone or electronic device, without getting a renewed FISA Court warrant.

It enables the government to keep track of suspected terrorists regardless of how many phones they use.

The target doesn’t have to be linked to a foreign power or terrorism, and the FISA Court doesn’t need to be told who’s being targeted when they issue a warrant.

The legislation could have been a lot worse.

Prior to Tuesday’s vote, Senate majority leader Mitch McConnell had tried to tack four amendments onto the Freedom Act that would have weakened key provisions of the bill, which the House of Representatives passed overwhelmingly last month.

The Senate shot down three of those amendments.

Namely:

A requirement that companies give the government 180 days notice before they could change data retention practices to keep call detail records for less than 18 months.

An amendment that would have stretched the effective date of the bill from six months to one year after enactment, thereby extending the NSA’s bulk collection program.

An amendment that would have gutted the bill’s accountability provision by limiting the duties and access of the public interest advocate and by removing the requirement that the Court provide written notice explaining when and why it chose not to appoint an amicus advocate.

The Electronic Frontier Foundation (EFF) clipped a clothespin over its nose so it could clap for the newly passed, sort of better surveillance law, which it says is a good start.

From the EFF’s Cindy Cohn and Mark Jaycox:

It’s no secret that we wanted more. In the wake of the damning evidence of surveillance abuses disclosed by Edward Snowden, Congress had an opportunity to champion comprehensive surveillance reform and undertake a thorough investigation, like it did with the Church Committee. Congress could have tried to completely end mass surveillance and taken numerous other steps to rein in the NSA and FBI.

It’s a lot easier to kill bad bills than it is to come up with good bills that protect people’s rights and can actually get through both the Senate and House of Representatives, they said.

The USA Freedom Act, for all of its warts, shows that the digital rights community can actually accomplish just that, they said.

Now that the legislation has neutered the phone records surveillance program and cracked the FISA Court to let in a bit of light and transparency, it’s time to turn to the task of tackling broader digital surveillance.

From the EFF:

We fought hard to get to this moment in history. Our long-term goals are ambitious - the end of overbroad surveillance of all digital communications, a recognition of the privacy rights of people outside the United States, and strong accountability and oversight for surveillance

practices. Today’s Senate vote did not accomplish these things, but it did move us a bit closer. ... It will also hopefully embolden Congress to feel that they can bring a sensible balance to surveillance policy and practice.

California Passes Law Requiring Warrant To Search Computers, Cellphones and Tabl ets

The hodgepodge of US state and federal laws about phone searches, some of which say that police need a warrant and some of which say they don’t, just got a bit messier.

As the LA Times reports, California on Wednesday joined the ranks of states that require police to have a warrant if they want to search computers, mobile phones, tablets and other devices, or if they want to siphon off location data from any of those devices.

The new bill, SB 178, was approved unanimously by California’s Senate.

The bill comes from Senator Mark Leno (D-San Francisco), who introduced a similar law two years ago.

Governor Jerry Brown vetoed that earlier version, saying that it was redundant with federal law and that the bill’s requirement that people be notified if their devices are searched would compromise criminal investigations.

The new bill addresses such concerns with a broad exception to the notification requirement when it could hamper an ongoing law enforcement investigation or jeopardise efforts to protect the public, Leno said.

SB 178 also provides exceptions for when the owner of a device gives consent to a search and when police believe that they need access to device information in the event of an emergency involving imminent danger of death or serious physical injury.

The LA Times quotes what Leno said to his colleagues about the law:

What the bill does is brings our state statute into the 21st century to catch up with technology with regards to privacy. Of course law enforcement needs a warrant before it can go into your mailbox and read your mail, but it does not currently need a warrant to read your emails or text communications or other electronic communications.

The other thing the bill does is align California with those states that have similarly ruled that phone records are constitutionally protected, including Montana, Maine, Minnesota, Massachusetts, and New Jersey.

Even with the broad exceptions stitched into the passed version of the law, prosecutors and police don’t like it.

The California District Attorneys Association, the California Police Chiefs Association and the California State Sheriffs Association have criticized it as being redundant with other privacy-protecting laws, as well as presenting roadblocks to investigations.

By proposing new procedures, the bill "undermines critical efforts to stop

child exploitation, mandates the destruction of evidence by law enforcement, and violates the California Constitution," the prosecutors group said in a letter to Leno that the Electronic Frontier Foundation (EFF) posted.

The sheriffs' group added that the bill...

...conflates existing procedures for obtaining certain electronic information under state and federal law, contains burdensome and unnecessary reporting requirements, and will undermine investigations that are fully compliant with the 4th Amendment.

The Feds have gone back and forth on this issue in recent cases, the most recent time siding with the prosecutors and police associations who criticized SB 178.

Last month, a federal appeals court ruled that police do not, in fact, need a warrant when seeking phone records from wireless carriers, thereby flip-flopping on its own decision from last year.

The reversal of the court's June 2014 decision left the question of warrantless phone tracking in limbo, with state courts and some higher courts coming to contradictory decisions.

Until the Supreme Court takes on the issue, someone living in California, or in any of the other states that now require a warrant for searching phone or other device data, is still facing a muddle of contradictory laws, regardless of what their state lawmakers have done to try to protect their privacy.

Violent Facebook Threats Conviction Thrown Out by US Supreme Court

His Facebook posts mused, among other things, about mass shooting school children, sticking his ex-wife's head on a stick, blowing up police stations, and slitting the throat of an FBI agent.

But on Monday, the US Supreme Court threw out the conviction of Anthony Elonis, saying that the fact that ordinary people would find such rants threatening isn't enough to convict people who make violent statements on Facebook and other social media.

What you also need in order to convict, the court ruled: to prove that there was actual intent, or that the person posting the threats thought that they'd be construed as actual threats.

Elonis's wife left the Pennsylvania man in 2010, taking their two kids with her.

Around the same time, he lost his job at an amusement park in Allentown, Pennsylvania.

That's when he began making threatening Facebook posts, including a comment on his sister-in-law's post about taking her niece and nephew (Elonis's son) trick-or-treating:

Tell [my son] he should dress up as matricide for Halloween. I don't know what his costume would entail though. Maybe [my ex-wife's] head on a

stick?

Elonis had adopted a pseudonym, "Tone Dougie", to post what he called his "rap lyrics" to Facebook, often interspersing then with disclaimers that the "lyrics" were fictitious and not intended to depict real persons, adding statements that said Elonis was exercising his First Amendment rights.

But many who knew Elonis saw his posts as threatening, including his boss, who fired him for threatening co-workers, and his wife, who sought and was granted a state court protection-from-abuse order against him.

In April, while the Supreme Court was poised to rule on whether he was wrongly imprisoned for his Facebook posts, Elonis was arrested after allegedly hurling a pot at his girlfriend’s mother when she tried to evict him, hitting her in the forehead and breaking her glasses.

Regarding the earlier case with the Facebook threats, a grand jury had indicted Elonis on five counts for making threats to injure patrons and employees of the amusement park, his then-estranged wife, police officers, a kindergarten class, and an FBI agent.

The Obama administration defended its prosecution of Elonis, saying that someone can be charged under a federal law as long as a reasonable person would view statements like these as a threat.

A Philadelphia-based federal appeals court upheld the conviction, and Elonis wound up serving more than three years of a 44-month sentence in prison.

When the Supreme Court agreed to take on an appeal, it marked the first time it’s ruled on people’s rights to post on social media - a potential free-speech landmark, given the enormous reach of online communication, the ability of thousands of people to instantly read postings, and the equally instant misinterpretations that can arise if such speech is taken out of context.

As it is, the First Amendment doesn’t protect anybody from saying anything they like.

Among the exceptions to protected speech covered by the First Amendment are true threats: i.e., those made with intent to carry them out.

In Monday’s decision, the Supreme Court found that the jury who convicted Elonis were given incorrect instructions when they were told they didn’t have to take his mental state into consideration.

Chief Justice John Roberts wrote in the opinion:

The jury was instructed that the Government need prove only that a reasonable person would regard Elonis’s communications as threats, and that was error.

In a 7-2 ruling, the court ruled to reverse the decision and hand the case against Elonis back to the lower courts.

The court noted that the mental state requirement would be satisfied if prosecutors could prove Elonis made the Facebook posts for the purpose of issuing a threat or with knowledge that they would be viewed as threats.

Dissenting opinions came from Justices Clarence Thomas and Samuel A. Alito Jr., who criticized the finding as causing more confusion instead of clarifying the First Amendment questions Elonis's case brought up.

From Justice Alito's dissent:

The Court refuses to explain what type of intent was necessary. Did the jury need to find that Elonis had the purpose of conveying a true threat? Was it enough if he knew that his words conveyed such a threat? Would recklessness suffice? The Court declines to say. Attorneys and judges are left to guess.

What Monday's decision means for lower courts is that they won't have a standard when trying cases, he wrote, which could lead to a bit of a mess:

If purpose or knowledge is needed and a district court instructs the jury that recklessness suffices, a defendant may be wrongly convicted. On the other hand, if recklessness is enough, and the jury is told that conviction requires proof of more, a guilty defendant may go free. We granted review in this case to resolve a disagreement among the Circuits. But the Court has compounded - not clarified - the confusion.

The Supreme Court avoided the conundrum by finding that criminal law in general, including the one used to convict Elonis, already requires a higher burden of proof when it comes to threats.

Roberts defended the limited decision, writing that it's sufficient to correct a misinterpretation by most lower courts that the poster's intent is immaterial and what matters only is how the message is received, and that the majority's prudence "is nothing new."

Civil libertarians are pleased with the limited ruling.
Advocates for victims of domestic abuse are not.

Steven R. Shapiro, legal director of the American Civil Liberties Union, told the Washington Post that the law has, for centuries, ... required the government to prove criminal intent before putting someone in jail. That principle is especially important when a prosecution is based on a defendant's words. The Internet does not change this long-standing rule.

Kim Gandy, president of the National Network to End Domestic Violence, told the newspaper that threats are a "core tactic" in domestic abuse:

Threats play a central role in domestic abuse and is a core tactic that many abusers employ. [Threats cause devastating harm] regardless of whether the abuser intended to threaten or only intended to vent or to make a joke.

It's hard to crawl inside somebody's head and suss out whether their threats reflect true intent, are meant as jokes, are artistic expression or are just the result of letting off steam.

That's why context is so important.

One example of courts apparently ignoring context came in the so-called "Twitter Joke" trial, which attracted attention within Great Britain and internationally when the UK's Royal Courts of Justice found that authorities went too far in prosecuting a man for threatening to blow

Nottingham’s Robin Hood airport "sky high" if his flight to Northern Ireland to visit his girlfriend was cancelled because of inclement weather.

The decision overturning the conviction said that the more one looked at it, the clearer it became that the message wasn’t a terrorist threat, let alone any form of threat, but rather was a shout-out to the man’s Twitter followers, drawing attention to his predicament.

In Monday’s ruling, the Supreme Court didn’t decide whether Elonis meant his threats or not.

That’s up to the lower courts to decide, using a different litmus test than they’d used before.

And thus we’re left, still, with the question of whether a man who’s been given a restraining order and has been arrested for assaulting a woman with a pan actually meant it when his Facebook postings suggested actions such as these:

There’s one way to love you but a thousand ways to kill you. I’m not going to rest until your body is a mess, soaked in blood and dying from all the little cuts.

[There are] enough elementary schools in a 10-mile radius to initiate the most heinous school shooting ever imagined. And hell hath no fury like a crazy man in a kindergarten class.

...and whether he should have been prosecuted and found guilty of illegal threats, or whether that would have been an assault on his First Amendment rights to free speech, if those posts are indeed simply rap lyrics.

The free-speech advocate in me applauds the court’s caution with regards to overzealous prosecutions of those who post threats on social media.

Still, it’s hard to be positive about a ruling that doesn’t seem to do much for those people who’ve been threatened online.

The Pirate Bay Co-Founder Released From Swedish Prison

Fredrik Neij, the third and the last founder of the infamous file-sharing website The Pirate Bay, was released on Monday from a Swedish prison.

Neij, who goes by the online moniker "TiAMO", was arrested by Thai immigration authorities at the end of November 2014 while he was trying to cross the border illegally from Laos to Thailand and then extradited to a prison in Skänninge, Sweden.

However, after his ten-month prison sentence, Neij is now a free man and has already reunited with family and friends, TorrentFreak reports.

The 37-year-old fugitive Swede man was first convicted of aiding copyright infringements by a Swedish court in 2009 and escaped arrest by fleeing to Laos.

However, Neji’s passport was revoked in 2012, and then after two years in November 2014, he was arrested under an Interpol warrant near the

Laotian border after four years on the run.

Before his arrest, Neji was living and hosting a file-sharing website called BayFiles, which was shut down afterwards.

All four co-founders of The Pirate Bay have now served prison sentences. The first Founder Gottfird Svartholm, who used the online alias "Anakata", was convicted on both copyright and computer hacking charges by a Danish court and is imprisoned, serving a three-and-a-half year sentence.

While the second founder, Peter Sunde served an eight-month sentence in Sweden last year. The Pirate Bay s financier Carl Lundström was also arrested and sentenced to four months of home arrest in 2012.

The Pirate Bay is a widely popular file-sharing website predominantly used to share copyrighted material free of charge, and despite the criminal convictions, the site remains functioning today, although it has moved to different Web domains several times.

It’s still unclear how the website managed to reappear every time after shutdown, but The Pirate Bay claimed last year that it ran the notorious website on 21 "raid-proof" virtual machines, which means if the police raid one location, the site would hardly take few hours to get back in action.

Neij is expected to return now to his house in Laos where he previously lived with his wife and children. TorrentFreak posted a picture of Neij "enjoying his freedom" with a beer cane in one hand. He is the last founder of The Pirate Bay to be released from prison.

Twitter Shuts Down Political Transparency Tool Politwoops

When US soldier and former Taliban POW Bowe Bergdahl was released last year, half a dozen politicians tweeted their "welcome home" messages and their thanks to a "true American hero."

Sometime between Bergdahl’s Rose Garden ceremony at the White House and the US Army charging him with desertion and misbehaviour before the enemy, those tweets popped out of public view like so many of those Anthony Weiner pics.

They didn’t entirely disappear from view, however, thanks to Politwoops, an archive of deleted tweets from US politicians that up until a few days ago was automatically following tweet deletions from the president, vice president, members of Congress, governors and anyone running for those positions.

In fact, here are those Tweets, preserved by Politwoops in spite of their creators having deleted them in an effort to back off from what had become politically embarrassing endorsements.

Many firmly believe that politicians and those running for public office, as public figures, have a different, lesser expectation of privacy than others on the Twitter platform, and that being able to see a politician’s flip-flopping is a valuable way to get some transparency into what they’re up to.

Twitter believes that too, it said recently, even as it killed Politwoops by yanking its access to Twitter's developer API.

That API had enabled the Sunlight Foundation-funded site to track the deleted tweets of hundreds of politicians.

A Twitter spokesperon provided this statement to Gawker on Wednesday:

Earlier today we spoke to the Sunlight Foundation, to tell them we will not restore Twitter API access for their Politwoops site. We strongly support Sunlight s mission of increasing transparency in politics and using civic tech and open data to hold government accountable to constituents, but preserving deleted Tweets violates our developer agreement. Honoring the expectation of user privacy for all accounts is a priority for us, whether the user is anonymous or a member of Congress.

It is true indeed that preserving deleted tweets goes against Twitter's developer agreement.

Here's what the Developer Agreement says about the matter:

Only surface Twitter activity as it surfaced on Twitter. For example, your Service should execute the unfavorite and delete actions by removing all relevant Content, not by publicly displaying to other users that the Tweet is no longer favorited or has been deleted.

The matter might seem cut and dried: Politwoops broke the rules, and Twitter pulled the plug.

But Twitter isn't coming out of this looking good, regardless of the slow clap it gave to Sunlight's mission.

As Sunlight Foundation President Christopher Gates said in his eulogy for Politwoops, the public service has been running since 2012: that's three years spent violating Twitter's developer terms, but doing so, apparently, with Twitter's blessing:

Days after Politwoops launched in 2012, Twitter contacted the Sunlight Foundation and told us, 'Your service violates our API Terms of Service on a fundamental level.' We explained the goals of the project and agreed to create a human curation workflow to ensure that the site screened out corrected low-value tweets like typos, links and Twitter handles. We implemented this layer of journalistic judgment with blessings from Twitter and the site continued.

Gates says Politwoops' staff is "truly mystified" at the change of heart but will honor Twitter's decision, even though...

It stands at odds with a fundamental understanding of our democracy. A member of Congress does not and should not have the same expectation of privacy as a private citizen. Power can only be accountable with a generous application of transparency.

After posting the news, Gawker received an anonymous email from someone claiming to be a Twitter employee with knowledge of the company's negotiations with the Sunlight Foundation.

Gawker says it can t verify whether the sender is actually employed by Twitter, so take the email with a grain of salt.

Here’s a version of the email that Gawker said it lightly edited for clarity:

I work at Twitter and am definitely a Politwoops fan despite knowing it violates our Terms of Service. (Definitely not in a decision making position though.) As you know, Sunlight had a phone call with a colleague here at Twitter. My understanding is, we were going to consider a quiet reversal but let s just say it didn t go well. (Lots of why us and not others.) And frankly I think we wound up digging in because of that. No More Politwoops :(:(. At least a few of us here still think that is a f*cking shame though.

The Washington Post’s Philip Bump, for one, calls Twitter’s move a "terrible decision."

While the Anthony Weiner sexting scandal came out of a vigilant watcher who was already suspicious of the politician, there’s plenty of room for an automated tool when it comes to keeping an eye on public figures, Bump notes:

Politwoops acted something like a campaign tracker: always there, always paying attention. Sometimes that can yield fake, biased news. Sometimes it can yield something that changes a political campaign. We need more services like Politwoops (as I’ve argued before), not fewer.

There are, in fact, ways around Twitter’s ban.

According to The Next Web, screenshots don’t violate developer agreements, even when automated.

But it sounds like the Sunlight Foundation, respectful of Twitter’s decision as it is, is above tricks like that.

And thus, we’ll have to see this window into political "oops!" tweets closed, and to witness transparency obscured because of it.

Microsoft’s Windows 10 Finally Has a Release Date

Microsoft has set a release date for Windows 10 to arrive in the summer.

The software maker announced Monday that it will begin offering its newest software to power PCs and tablets as a free upgrade on July 29. Windows 10 Mobile, the company s companion software designed to power smartphones, is expected to arrive later this year. Windows 10 will be free for users who have bought a computer in the past six years or so, powered by Windows 7 or later, or tablets running Windows 8.1.

Windows 10 marks the next iteration of the one of the world s most ubiquitous pieces of software. Microsoft s operating system powers a majority of personal computers and acts as the backbone of many of the world s businesses. Despite its dominance, Microsoft critics see the company and its products as a tech titan in decline, as mobile phones and competing, cheaper software have chipped away at Windows. The company s goal with Windows 10 is both to repair the damage done by the ill-received Windows 8 and convince consumers that upgrading is worth the time and effort.

Rumors originally swirled around a July release date for Windows 10 back in April when Lisa Su, head of chipmaker AMD, discussed the timeline on a conference call. Microsoft has mostly remained mum, however, coyly avoiding discussion of a launch date even during its developer conference in April. Some industry watchers became concerned the software may not be ready in time.

Microsoft has not disclosed when computer makers will begin selling PCs pre-loaded with Windows 10 or when retailers will sell individual licenses in the event you are not eligible for a free upgrade or wish to build your own computers. However, a leak from online retailer Newegg on Saturday indicated that PC makers would receive the software August 31. Newegg also leaked screenshots revealing that the software sold on its own would cost hardware makers $109, while the Professional version will run $149, according to the listings, which were first spotted by ZDNet.

Through its Windows Insider program, which lets eager users sign up to receive developer versions of the software-in-progress, Microsoft has been more transparent with Windows 10 than previous releases. Since its unveiling in September, interested users have watched the software s evolution firsthand. Some of the key changes Microsoft has made include a revamped Start button and the removal the unpopular tablet-focused interface of Windows 8. There s also a new browser, Edge, to replace the decades-old Internet Explorer, as well as a more robust version of Cortana, Microsoft s voice-enabled digital software assistant.

The most important aspect of Windows 10, however, is the company s philosophy powering it: one Windows to rule them all.

Microsoft remains the world s largest software maker with Windows running on more than 90 percent of the world s computers, according to NetMarketShare. But the company had a late start on smartphones and has struggled to keep its software relevant while developers focused on Apple s iOS mobile operating system, Google s Android and the Web at large. PCs sales have also been on a steady decline.

With Windows 10, Microsoft is making a big gamble that its Windows software can power a web of devices, attracting customers to own computers, tablets and smartphones all powered by one company s software. It s a gamble that s worked for Apple, whose iPhones, iPads and Macs are well regarded for working well with one another.

Microsoft executives, including CEO Satya Nadella, have stressed the importance of thinking of Windows and Microsoft software as services, not products we buy. The company s already begun applying this model to its Office software suite, which includes programs like Word, Excel and Outlook. Microsoft now available offers it as subscription service, called Office 365, instead of selling individual disks to customers at a one-time flat rate.

The company has not yet said if there will ever be a Windows 11, or a version of Windows we consumers will pay for like past releases. Users who update to Windows 8 will get new features and benefits for a long, long time, said Joe Belfiore, Microsoft s vice president of operating systems, said at Build earlier this month.

Though it still makes most of its money selling its traditional software to businesses, Microsoft s fastest growing business division is its cloud services group, which is on track to make $6.3 billion in sales this

year. Nadella, who oversaw Microsoft s cloud business before assuming the role of chief executive in February 2013, hopes to see annual sales there grow to $20 billion over the next three years.

By 2018, Microsoft hopes to have more than 1 billion devices running Windows 10. That s ambitious, particularly considering Microsoft s previous release, Windows 8 which arrived in 2012, powers less than 15 percent of the world s computers.

Microsoft Prices Windows 10 Licenses at $119 for Home, $199 for Pro

Microsoft has a grand plan to get its next operating system, Windows 10, running on 1 billion devices in three years - by giving it away for free. Well, sort of.

The software, which Microsoft announced Monday will begin rolling out July 29, will be offered as a free upgrade for all Windows 7 and Windows 8.1 PC and tablet users. For the PC market, those two versions power 74.1 percent of all devices, according to NetMarketShare.

For everyone else, Windows 10 will cost the same as its predecessor, Windows 8, the company confirmed to CNET on Monday.

A copy of Windows 10 Home will run $119, while Windows 10 Pro will cost $199. For those who wish to upgrade from the Home edition to the Pro edition, a Windows 10 Pro Pack will cost $99.

Microsoft may have given the impression it was making a critical pricing change to its flagship operating system when it announced in January that, like competitor Apple, it would offer an upgrade free of charge. However, the company has been transparent from the beginning that the upgrade is only eligible for one year, until July 29, 2016, and has said at various points in the past few months that pricing for single licenses would stay on par with previous releases. Now, there is the possibility that future versions of Windows may follow this same path, meaning Microsoft may never go fully free with its OS.

Microsoft says copies of the software will be available online and in stores. Retailer Newegg, which appeared to have leaked pricing and release date information this past weekend, still has pages for Windows 10 Home and Pro live on its website, although its pricing says $110 for Home and $150 for Pro and is not updated to reflect Microsoft’s confirmed pricing.

For those eligible for the free upgrade, the process will only grant you an equitable version of the software. That means if you had Windows 7 Home, you get Windows 10 Home. If you had Windows 8.1 Pro, you get Windows 10 Pro. See here for more details. For more information on how to check your upgrade eligibility and reserve your upgrade for the July 29 rollout, check out CNET’s guide.

As for why one would be buying Windows 10 in the first place, single licenses are useful for the minority of users who don’t have an eligible machine or wish to build their own computer in the coming months and install Windows themselves.

Finally: A Service That Lets You Charge People To Email You

If I were to charge people to email me, I could likely retire before the year is done. I get more than 100 emails per day on a slow day, and my inbox can easily top 200 emails on a busy day. This, of course, is why I had no choice but to destroy email.

Of course, it wouldn t be ethical for me to charge companies to pitch me, so I would never use a service like Wrte.io. For others out there without ethical barriers, however, a service that lets you charge people to email you might just be your new favorite thing in the world.

Wrte.io is brilliantly simple and simply brilliant. It works like this: You get a special @wrte.io email address and either give it out to people as your main email address or just forward messages from your current account to that address. When someone emails you at that new address, he or she automatically gets a reply that states how much it costs to email you and includes a link to a simple payment gateway where the person can pay by credit card or bitcoin.

Once the payment is verified, the email is forwarded to your personal email address. The money paid to send you that email will then be deposited in your Stripe account or donated to charity via Watsi, if you prefer. The service charges a fee that varies depending on how much you charge to receive emails.

Wrte.io is currently in open beta and anyone can sign up.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.